The Ultimate Guide to Securing Magento Admin

Powred By :

NextBits

OVERVIEW

Preserving website security, particularly for the e-commerce website is an ever growing challenge for on-line retailers. Maintaining website security with developing security standards is one of the essential for the website.

This document focuses primarily on suggested steps for securing a Magento Store by looking at critical aspects of Admin Account and secret Management.

We discussing admin credential management, as that is most common and easy way for any individual to access Magento Store and insert malicious code or get access to customers information.

By login to an administrator account, a hacker can gain access to a Magento store, add a module to change the code, and with inserted code gain access to sensitive info. All without triggering any red flags to Network, Hosting and Code managers. This reason alone is why it's important to use business practices that can avoid this sort of vulnerability.

The most recent version of the Payment Card Industry Security Standards (PCIDSS) Version 3.1 published on April 2015 and downloadable via this link: **https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf** provides the complete list of standards that merchants and e-commerce service providers should follow. In this paper, we are sharing few basic things that are high yield recommendations which will help you to reduce your Magento store's vulnerabilities.

1. Avoid poor credentials for admin account

Do you remember when you change the password for your Magento administration account? if your answer is "NO", then you should change it today.Make sure you don't set a weak password like your pet name, the name of a favorite sports team, your company name + the year, or a date of significance (like birthday, anniversary). you should choose a strong password which should be min. 8 character long having the random combination of uppercase-lowercase letters, numbers and special characters. Having a strong password can secure your site against brute-force attack too.
Do you remember when you change the password for your Magento administration account? if your answer is "NO", then you should change it today.Make sure you don't set a weak password like your pet name, the name of a favorite sports team, your company name + the year, or a date of significance (like birthday, anniversary). you should choose a strong password which should be min. 8 character long having the random combination of uppercase-lowercase letters, numbers and special characters. Having a strong password can secure your site against brute-force attack too.

2. Share details with Trusted Admins only

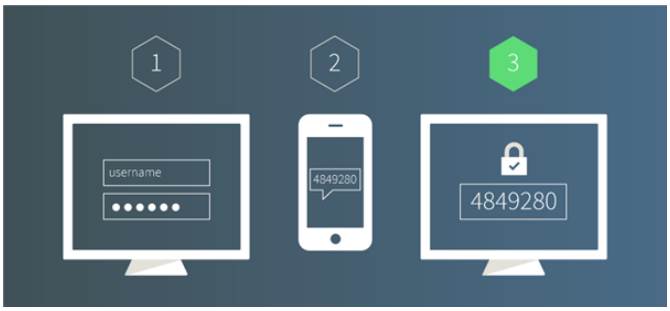
A potential vulnerability with e-commerce store is losing Admin control. This risk can occur with straightforward oversights like the employee who left the company recently (who know the credentials), or providing credentials to a developer that has

to support you with the installation of the most recent and greatest extension, we recommend not to give Administrator passwords to extension developers. we also suggest you remove unnecessary admin accounts.

3. User Roles

Not everybody needs an Administrator privileges. That is true that some users need full access of the backend. There are many user roles that need access of a subset of functionality. For example, Customer Support Representatives don't need the ability to install new extensions. Magento has an incredible capability to configure user roles.you can create user different roles and give access permission to them as per user requirements.

4. Use Two Factor Authentication



What is Two-Factor Authentication? Two-factor authentication is the combination of at least two different validation methods during any single authentication request.

This will an additional security step for login in the admin area. The user needs to add a one time security code. There are extensions available for Magento you can buy one of them and install it on your Magento store to enable two factor authentication.

https://www.magentocommerce.com/magento-connect/two-factor-authentication-by-amasty.html

5. Use IP Lookup

Hackers can try to login to Magento admin with your stolen passwords. we can restrict them. with IP lookup, you can allow some specific IPs (whitelisted IPs) to access the back-end. so if anyone try to access Magento backend who's IP is not in whitelist then he can not access the backend. there are ready made Free extensions available in the market-place you can download and install it to your Magento website. you can also decide whether to allow visitors from specific country and block from other.

https://www.magentocommerce.com/magento-connect/et-ip-security.html

6. Admin Logging

Be aware of how, when, by whom your store data has been accessed and modified. See all the actions performed by you and other admin users in the store backend. Why is it so important to track admin action? suppose something went wrong in your store, and you really need to see who had made these changes. Using Magento admin actions log Now you can just open Magento admin actions log and find this out. Moreover, you can con-trol the managers of your store more efficiently when you see the actions they perform.

Periodic log reviews are an important part of any good security program. While they won't prevent a user with an admin account from installing a trojan horse extension, it will help you to identify when a change has been made and the account that made it.

https://www.magentocommerce.com/magento-connect/admin-actions-log-by-amasty.html
https://www.wyomind.com/security-enhancement-magento.html

7. Use a custom admin path

In most of the Magento site, you can access your Magento admin area by going to yoursite.com/admin. Easily accessible admin area makes an easy task for hackers to access it and try various password directly. A custom path admin panel can secure admin area and can prevent users from them to reach admin area. Magento security experts also suggest to use custom path for backend instead of using a common path like yoursite.com/admin.
you can change admin path from your Magento
`Admin panel > System > Configuration > Advance Menu > Admin section`
under the Admin Base URL OR you can change it app/etc/local.xml
In the local.xml file you will find the following block of code:

```
<admin>
   <routers>
      <adminhtml>
         <args>
            <frontName><![CDATA[admin]]></frontName>
         </args>
      </adminhtml>
   </routers>
</admin>
change
<frontName><![CDATA[admin]]></frontName>
```

8. Use secure FTP (SFTP)

There are possibilities that hackers may hack your site via your FTP. In order to prevent unauthorized access to your website's FTP, you should use secure passwords and use SFTP (SSH File Transfer Protocol) or FTP-SSL(Explicit AUTH TLS). Public Key Authentication with SFTP can increase security even more by requiring a private key file and an optional description password to authenticate the FTP access.

9. Site Security Monitoring

Beyond some of the straightforward changes, we have identified. we also recommend ongoing monitoring of Website security vulnerabilities.
Solutions from sucuri.net allow you to Security Analysis, Malware Scanning and Detection, Repair Dirty SEO, Security Monitoring, Distributed Denial of Service DDoS) Mitigation, Stop Website Attacks and Hacks and more.

10. Keep Magento Updated with latest Patches

Magento releases Security patches to secure your Magento websites and prevent hacks and cover any loopholes in the existing in Magento. If your site has not been patched, we strongly urge you to install all the security patches and secure your Magento website.you may want to know how can you check which security patches your Magento site need to be implemented? At https://www.magereport.com/ you can Scan and check your Magento shop for known security vulnerabilities. The scan will give you a detailed report regarding patches which are successfully applied and patches and other issues need to address.

Conclusion:

security is one of the critical and essential concern for any eCommerce website. Fundamental step to secure any eCommerce website is to secure your Admin accounts.
No matter how good your website security or your infrastructure security, if you don't have a solid approach to managing and securing your admin accounts, you are at risk of a security breach.